ISSN 2007-9737

Financial Fraud Detection in the Banking Sector Using Machine Learning: An Exhaustive Systematic Review

Orlando Jeri-Alvarado[1], Cristopher Espinoza[1], Javier Gamboa-Cruzado[2], María León Morales[3], Victor Ataupillco-Vera[2], Oscar Chávez-Chavez[2], Carlos Andrés Tavera Romero[4], Francisco Antonio Castillo-Velázquez[5,*]

[1] Universidad Nacional Federico Villarreal,
Peru

[2] Universidad Nacional Mayor de San Marcos,
Peru

[3] Universidad Nacional de Cajamarca,
Peru

[4] Universidad Santiago de Cali,
Colombia

[5] Universidad Politécnica de Querétaro,
Mexico

2022016416@unfv.edu.pe, 2022016283@unfv.edu.pe, jgamboac@unmsm.edu.pe, mleon@unc.edu.pe, vataupillcov@unmsm.edu.pe, oscar.chavez1@unmsm.edu.pe, carlos.tavera00@usc.edu.co, francisco_velasquez@yahoo.com.mx

Abstract. In recent years, the application of machine learning techniques for detecting financial fraud within the banking sector has experienced a remarkable increase. This paper seeks to highlight this progress and emphasize its impact on enhancing fraud prevention and control systems. The objective of this paper is to explore, determine, and identify the current state of knowledge regarding the use of machine learning in financial fraud detection in the banking sector. This study was based on 61 papers selected from six major digital libraries: IEEE Xplore, Scopus, ScienceDirect, ProQuest, ARDI, and Web of Science. Only peer-reviewed journal papers were included. The systematic review covered publications between 2019 and 2025, available in open-access databases, focusing on the use of machine learning in detecting financial fraud in the banking sector. The findings from the 61 reviewed papers indicate that the most widely used programming language for machine learning solutions is Scala. Additionally, tools implemented in fraud detection and gaps in model comparison were identified. It is recommended to explore more recent approaches and banking contexts that have not yet been addressed.

Keywords. Financial fraud detection, banking sector, deep learning, identification of financial scams.

1 Introduction

In the digital era, financial fraud has become one of the main threats to the integrity and stability of the banking sector. In this scenario, machine learning has emerged as a key tool to strengthen fraud detection and prevention mechanisms, due to its ability to analyze large volumes of data and identify anomalous patterns in real time. This technology provides a proactive approach that overcomes the limitations of traditional methods. Therefore, it is essential to understand the current state of knowledge in this area. This paper conducts a systematic review of recent literature to identify advances, commonly used approaches, and existing gaps in the application of machine learning to banking fraud detection. This study presents a framework to integrate fairness and transparency into machine learning models such as LightGBM and XGBoost applied to financial and real estate data. It employs fairness techniques such as Calibrated Equalized Odds and SHAP to enhance transparency, underscoring the

doi: 10.13053/CyS-29-3-5909

importance of responsible practices in critical financial decision-making [1]. The paper also proposes an integrated Blockchain and Artificial Intelligence (IBAI) framework for secure financial transactions, protecting confidential data in untrusted networks. Blockchain stores centralized data, while AI analyzes and detects suspicious behavior, increasing detection accuracy to 98% compared to other models [3]. The sophistication of fraud surpasses traditional detection methods, exposing banks to financial risks. This study proposes an Explainable Federated Learning (XFL) model that combines privacy and transparency, achieving 99.95% accuracy in fraud detection. It incorporates SHAP and LIME to improve explainability and regulatory compliance [4].

The RXT model, based on GRU and ResNeXt, addresses financial fraud through real-time data processing. It employs SMOTE to balance data and EARN for feature extraction. Optimized with Jaya, it outperforms existing algorithms by 10%–18% across three datasets, enhancing both financial security and efficiency [5]. Another study analyzes money laundering detection in Saudi Arabia using supervised learning. Four algorithms (RF, DT, GB, KNN) were evaluated with data from 2016–2019, with RF achieving 93% accuracy at the establishment level, thereby improving proactive detection and supporting the Financial Intelligence Unit [6]. Financial fraud detection requires effective machine learning models. The Voted Perceptron (VP) model enhances detection by dynamically adapting to changing patterns, surpassing traditional models such as KNN and Naïve Bayes. VP achieves lower error rates and greater adaptability, standing out in both accuracy and flexibility [8].

An innovative hybrid model combining machine learning and deep learning techniques is proposed for detecting fraud in banking transactions. Using a stacking method, the model improves predictive accuracy, achieving an F1 score of 94.63%, highlighting its effectiveness in cyber fraud detection [9]. Another paper introduces a novel algorithm to detect fraudulent accounts in large-scale banking transaction graphs. It applies a three-step parallel approach and demonstrates high efficiency and scalability on multicore processors, contributing to combating financial fraud and promoting stability in the banking sector [10]. FraudGNN-RL is an innovative framework that combines Graph Neural Networks and Reinforcement Learning to detect financial fraud. It models transactions as a dynamic graph and uses a novel architecture to capture temporal, spatial, and semantic patterns.

It outperforms current methods, achieving a 97.3% F1-score and reducing false positives by 31% [11]. The increase in credit card fraud and the effectiveness of machine learning techniques to detect it are also examined. The study reviews papers from five databases, identifying research gaps and future opportunities. It concludes that the field has gained significant relevance over the past decade, with both supervised and unsupervised techniques standing out [12].

Data privacy is crucial in the financial sector to protect sensitive information. One study proposes a hierarchical hyperparameter optimization approach using machine learning to classify network intrusions with the CICIDS 2017 dataset. LGBM achieved 99.77% accuracy in detecting DDoS attacks [13]. Detecting anomalies in high-value payment systems (HVPS) is challenging due to the large volume and scarcity of anomalous payments. These systems are critical to national financial infrastructure, and their protection requires real-time monitoring amid growing cyber threats [14].

Another study explores the application of machine learning in banking fraud detection, highlighting advanced algorithms (CART, Gradient Boosting, XGBoost) tested on 1.5 million transactions. Their effectiveness in handling imbalanced data is emphasized, providing valuable insights to improve financial security and risk management [16]. Research has also analyzed the adoption and impact of artificial intelligence and machine learning in financial markets, using surveys and qualitative methods. Applications such as algorithmic trading and risk management are highlighted, along with challenges, trends, and ethical considerations, stressing the need for professional adaptation and regulatory compliance [17].

Financial fraud has increased with technological advancements, costing billions annually. Current methods are insufficient, underscoring the need for post-fraud detection systems. Anomaly detection techniques, particularly semi-supervised and unsupervised learning models, have advanced to address this issue, according to recent studies [21]. Another paper proposes a credit governance method integrating IoT technology and an enhanced Long Short-Term Memory model.

The model automatically adjusts parameters to improve performance, achieving high classification accuracy with values of 0.9 for precision, 0.91 for F1, and 0.94 for AUC in experimental tests [22]. Credit card fraud detection is vital for financial security. A model based on Quantum AutoEncoders (QAE-FD) is proposed to improve anomaly detection. Tested on a real dataset, it achieved a G-mean of 0.946 and an AUC of 0.947, outperforming existing models in both accuracy and computational efficiency [23].

The digitization of payments has further increased financial fraud. A study applied machine learning models such as Isolation Forest and autoencoders in a Greek bank to detect anomalies in an unsupervised manner. Autoencoders proved especially effective. Genetic algorithms and SHAP were used to improve feature selection and interpretability [25]. Another investigation explored the use of deep learning in fraud detection, employing Graph Neural Networks and Autoencoders. Validated in banking contexts, these models enhanced the accuracy and efficiency of real-time banking systems. Python was used for analysis, demonstrating the ability to handle dynamic fraud [26].

Credit card fraud detection faces significant challenges. One study compared Kolmogorov-Arnold Networks (KAN) with Multilayer Perceptrons (MLP), highlighting that KAN outperformed MLP in accuracy and parameter efficiency. The results suggest that KAN provides more effective and interpretable solutions for fraud detection [29]. An improved R-GAN model is also proposed for real-time financial fraud detection, addressing data imbalance through synthetic generation and explainability with SHAP [31]. Another study evaluated machine learning models for detecting financial statement fraud, highlighting the strong performance of XGBoost and SVM, and the importance of key accounting indicators in interpretation [32]. An intelligent system is proposed for credit card fraud detection, combining deep learning techniques and bio-inspired optimization, achieving better results than previous approaches [34].

Additional research developed machine learning models for banking fraud detection, emphasizing preprocessing techniques and showing that neural networks and ensemble methods significantly improve accuracy [39]. A sequential deep learning-based model is proposed to classify financial transactions, integrating ensemble learning and temporal pattern extraction, achieving high precision in fraud detection [41].

Financial fraud detection using machine learning is largely based on supervised models and real-world data, with a strong focus on credit card fraud. Among 104 reviewed studies, fewer than 7% used synthetic data. China, India, and Canada lead research in this area, while Latin America shows limited participation [65]. Another review of 93 papers on financial fraud detection using machine learning highlighted SVM and neural networks. Credit card fraud was the most studied type, with common metrics such as accuracy and F1-score, while gaps remain in explainability methods and data quality [71].

A systematic review of 57 studies applying deep learning to financial fraud emphasized models such as CNN, LSTM, Transformers, and GNN in contexts like credit cards and insurance. Challenges such as imbalanced data and interpretability were addressed through techniques such as SMOTE, GANs, and blockchain [70]. Another study analyzed statistical, machine learning, and hybrid techniques for detecting financial statement fraud, employing models such as XGBoost, LSTM, Node2Vec, and NLP applied to financial and textual data. The importance of preprocessing, variable selection, and regulatory compliance was highlighted [69]. AI-based methods for fraud in public procurement have also been reviewed. Algorithms such as Random Forest, SVM, neural networks, and graph analysis were applied to open data, addressing issues such as corruption and collusion, with tools including Python, Neo4j, and KNIME [75].

A bibliometric analysis of 26 papers on crowdfunding platform fraud highlighted algorithms such as Random Forest, SVM, and ANN, identifying fraud types such as fake campaigns and

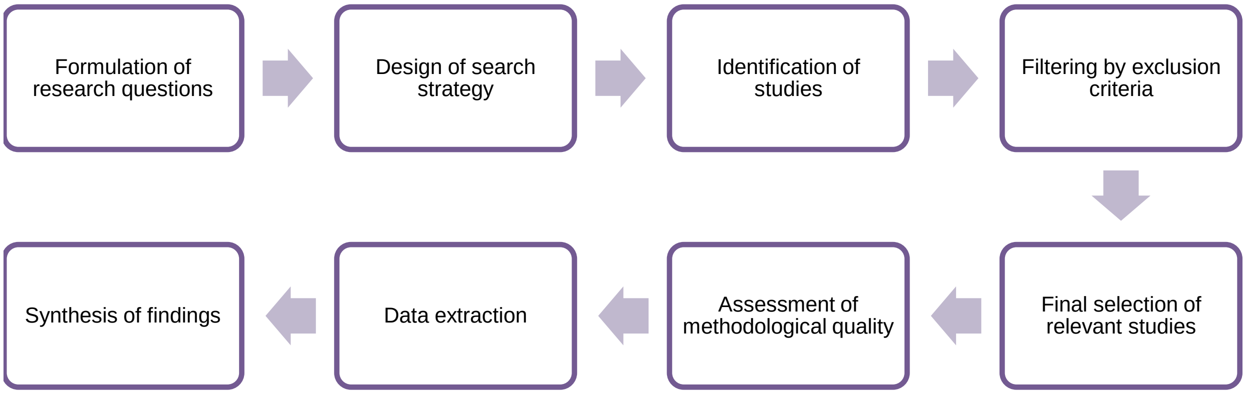

Formulation of research questions
Design of search strategy
Identification of studies
Filtering by exclusion criteria
Final selection of relevant studies
Assessment of methodological quality
Data extraction
Synthesis of findings

Fig. 1. Step-by-step description of the systematic literature review protocol

Table 1. Research Questions and Their Objectives

Research Question (RQ)	Objective
RQ1: What are the criteria for measuring the effectiveness of Machine Learning in detecting financial fraud in the banking sector?	To determine the criteria for measuring the effectiveness of Machine Learning in detecting financial fraud in the banking sector.
RQ2: What programming languages are most commonly used in the development of Machine Learning solutions?	To identify the programming languages most commonly used in the development of Machine Learning solutions.
RQ3: What are the quartile levels of the journals that have published research on the effect of Machine Learning in detecting financial fraud in the banking sector?	To classify the quartile levels of the journals that have published research on the effect of Machine Learning in detecting financial fraud in the banking sector.
RQ4: What thematic categories are presented in research on Machine Learning and its impact on detecting financial fraud in the banking sector?	To classify the thematic categories presented in research on Machine Learning and its impact on detecting financial fraud in the banking sector.
RQ5: What are the most frequently used concepts, by year, in research on the use of Machine Learning and its impact on detecting financial fraud in the banking sector?	To explore the most frequently used concepts, by year, in research on the use of Machine Learning and its impact on detecting financial fraud in the banking sector.

fund misappropriation. The United States, Germany, and Canada lead this area, with no significant differences among institutions [74]. Another bibliometric study analyzed 189 papers on machine learning in finance since 1988, highlighting its growth since 2017.

The most common applications are prediction, crowdfunding, and fraud detection. The U.S., China, and the U.K. dominate scientific production, although international collaboration remains limited, and interdisciplinary gaps persist [68]. Artificial intelligence is transforming the financial sector, applying machine learning and NLP in areas such as credit scoring, fraud detection, and robo-advisory. Although operations are optimized, implementation faces major ethical and regulatory challenges, with a lack of standardized frameworks.

A balance between innovation and strong governance is required [81]. A bibliometric analysis of 706 papers identified trends in digital fraud and financial crimes. Four main themes emerged: e-commerce risk, AI-based prevention, digital banking behavior, and cybersecurity. Research has expanded since 2015, with a focus on blockchain, digital signatures, and machine learning [78]. Another systematic review of 66 papers examined machine learning in e-commerce, focusing on its impact on service personalization, price optimization, and fraud

Table 2. Search terms and their synonyms

Descriptor	Description
machine learning/ ml/ deep learning/ artificial intelligence/ ai	Independent Variable (A)
detection/ identification/ recognition/ monitoring/ finding + financial fraud/ financial scam + banking sector/ banking system/ financial sector	Dependent Variable (B)

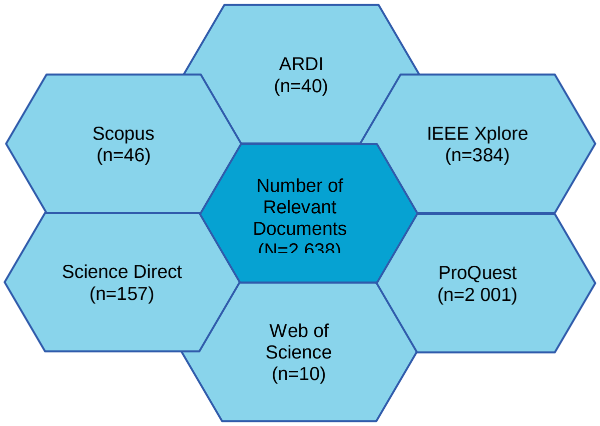


Fig. 2. Compilation of retrieved documents

detection. Emerging techniques such as Graph Neural Networks and federated learning were identified, though challenges such as geographic bias, model overfitting, and the lack of standardized datasets persist. The study recommends improving evaluation in real-world contexts [66].

A systematic review in this field is essential to understand how machine learning techniques are being applied to banking fraud detection, a problem that is becoming increasingly complex and frequent. This synthesis will allow the identification of effective approaches, research gaps, and current trends, providing a useful basis for both researchers and financial sector professionals interested in strengthening detection systems through AI-based solutions. Although multiple studies exist on machine learning applied to financial fraud detection, the literature reveals significant gaps, such as the lack of comprehensive perspectives beyond credit card fraud, as well as challenges in handling imbalanced data and ensuring model explainability. Moreover, emerging approaches—such as federated learning, graph neural networks, and hybrid models with Blockchain—still lack critical systematization to fully understand their real scope. Therefore, a systematic review is justified to synthesize the most relevant approaches, identify trends and gaps, and provide an updated framework that guides both future research and practice in the banking sector.

Accordingly, the objective of this review is to examine the current state of knowledge on the application of machine learning to financial fraud detection in the banking sector. Within this framework, the paper is structured as follows: Section 2 presents the theoretical background; Section 3 describes the methodology; Section 4 discusses the main results; and Section 5 offers the conclusions along with potential future research directions.

2 Background

The growing advancement and adoption of machine learning in the financial domain, particularly in banking fraud detection, makes it necessary to review the fundamental concepts that support its application. In this regard, the following theoretical background is presented as the basis for better understanding the approach and scope of this systematic review.

2.1 Machine learning

Studies reveal the influence of artificial intelligence and machine learning in financial markets, highlighting, on the one hand, adoption trends in algorithmic trading and regulatory risk management [17]. Likewise, deep learning with Graph Neural Networks of Lambda architecture and autoencoders facilitates real-time fraud detection, achieving an appropriate balance between precision and recall in dynamic banking systems [26].

Similarly, machine learning has been applied to financial statement classification using Decision Tree, SVM, Random Forest, and XGBoost, where the use of SMOTE allows key ratios (IBD/TIC, QR) to be emphasized in the detection of corporate fraud [32].

Conceptually, machine learning is defined as a branch of artificial intelligence that enables systems to learn from historical data to predict outcomes without the need for explicit programming [82].

Furthermore, it constitutes an evidence-based proactive approach that anticipates errors through automated internal analyses, optimizing decision-making in organizational processes such as API and software deployment [76].

Finally, it can be understood as a set of techniques designed to allow systems to automatically learn from data, with the goal of optimizing processes and improving decision-making in complex environments such as Software-Defined Networks (SDN) [77].

2.2 Financial Fraud Detection in the Banking Sector

The detection of financial fraud in the banking sector, which negatively affects administrative and organizational processes, has been increasingly addressed through machine learning techniques [65]. With the advancement of artificial intelligence, these approaches allow the identification of fraudulent transactions through the analysis of large volumes of financial data [71], and have progressively incorporated deep learning methods that have demonstrated significant improvements in detection accuracy [70].

The complexity of financial markets, together with the growing availability of data, makes anomaly detection in financial statements a critical challenge that demands robust and scalable models [69]. In this context, artificial intelligence techniques—including machine learning and natural language processing—have been adopted to more effectively address the problem of fraud [75]. Particularly relevant is the detection of fraud in online credit card transactions, considered an urgent global socioeconomic challenge that drives the development of solutions based on machine learning, deep learning, and ensemble approaches [79].

2.3 Tools Used

For the development of this research, **Mendeley Desktop** was employed as the reference manager, enabling efficient organization and management of the reviewed papers. Likewise, the analytical charts presented in the results and discussion sections were produced with the support of the research assistant **RAj**, a tool developed by Dr. Javier Gamboa Cruzado, which facilitated data processing and visualization.

3 Methodology

This work was conducted following a Systematic Literature Review (SLR) methodology, primarily based on the guidelines of Kitchenham and Charters [62], who established a rigorous and reproducible approach for the collection, evaluation, and interpretation of scientific evidence, particularly tailored to software engineering. As a complement, the updated recommendations of Petersen and colleagues [63] were also considered, as they emphasize improvements in the structure of the processes for study search, selection, and categorization, incorporating consolidated practices derived from multiple empirical studies.

This methodological combination allowed the analysis to be organized in an orderly, rigorous, and reliable manner, structuring the process into three stages: planning, execution, and reporting of results.

Figure 1 schematically illustrates the workflow followed in this research, covering the entire process from the formulation of the initial research questions to the synthesis of the main findings.

3.1 Research Questions and Objectives

As presented in Table 1, this study formulates several research questions (RQs) that allow for a structured examination of different aspects of the topic. This distinction strengthens methodological rigor by guiding both the search strategy and the interpretation of the literature, ensuring a clear and well-founded synthesis of the findings.

Table 3. Search Equations by Source

Source	Search Equation
Scopus	((TITLE("machine learning") OR TITLE("ml") OR TITLE("deep learning") OR TITLE("artificial intelligence") OR TITLE("ai")) AND (TITLE("detection") OR TITLE("identification") OR TITLE("recognition") OR TITLE("monitoring") OR TITLE("finding")) AND (TITLE("financial fraud") OR TITLE("financial scam") OR TITLE("banking fraud")) AND (TITLE("banking sector") OR TITLE("banking system") OR TITLE("financial sector"))) OR ((KEY("machine learning") OR KEY("ml") OR KEY("deep learning") OR KEY("artificial intelligence") OR KEY("ai")) AND (KEY("detection") OR KEY("identification") OR KEY("recognition") OR KEY("monitoring") OR KEY("finding")) AND (KEY("financial fraud") OR KEY("financial scam") OR KEY("banking fraud")) AND (KEY("banking sector") OR KEY("banking system") OR KEY("financial sector")))
IEEE Xplore	("Document Title":"machine learning" OR "Document Title":"ml" OR "Document Title":"deep learning" OR "Document Title":"artificial intelligence" OR "Document Title":"ai") AND ("Document Title":"detection" OR "Document Title":"identification" OR "Document Title":"recognition" OR "Document Title":"monitoring" OR "Document Title":"finding") AND ("Document Title":"financial fraud" OR "Document Title":"financial scam") AND ("Document Title":"banking sector" OR "Document Title":"banking system" OR "Document Title":"financial sector") OR ("Author Keywords":"machine learning" OR "Author Keywords":"ml" OR "Author Keywords":"deep learning" OR "Author Keywords":"artificial intelligence" OR "Author Keywords":"ai") AND ("Author Keywords":"detection" OR "Author Keywords":"identification" OR "Author Keywords":"recognition" OR "Author Keywords":"monitoring" OR "Author Keywords":"finding") AND ("Author Keywords":"financial fraud" OR "Author Keywords":"financial scam") AND ("Author Keywords":"banking sector" OR "Author Keywords":"banking system" OR "Author Keywords":"financial sector")
Web of Science	TI=("machine learning" OR "ml" OR "deep learning" OR "artificial intelligence" OR "ai") AND ("detection" OR "identification" OR "recognition" OR "monitoring" OR "finding") AND ("financial fraud" OR "financial scam") AND ("banking sector" OR "banking system" OR "financial sector") OR AK=("machine learning" OR "ml" OR "deep learning" OR "artificial intelligence" OR "ai") AND ("detection" OR "identification" OR "recognition" OR "monitoring" OR "finding") AND ("financial fraud" OR "financial scam") AND ("banking sector" OR "banking system" OR "financial sector")
ProQuest	(TI("machine learning" OR "ml" OR "deep learning" OR "artificial intelligence" OR "ai") AND TI("detection" OR "identification" OR "recognition" OR "monitoring" OR "finding") AND TI("financial fraud" OR "financial scam") AND TI("banking sector" OR "banking system" OR "financial sector")) OR (SU("machine learning" OR "ml" OR "deep learning" OR "artificial intelligence" OR "ai") AND SU("detection" OR "identification" OR "recognition" OR "monitoring" OR "finding") AND SU("financial fraud" OR "financial scam") AND SU("banking sector" OR "banking system" OR "financial sector"))
Science Direct	("machine learning" OR "deep learning" OR "artificial intelligence") AND ("financial fraud" OR "financial scam") AND ("detection" OR "monitoring") AND ("banking sector" OR "financial sector")
ARDI	((Title:"machine learning" OR Title:"ml" OR Title:"deep learning" OR Title:"artificial intelligence" OR Title:"ai") AND (Title:"detection" OR Title:"identification" OR Title:"recognition" OR Title:"monitoring" OR Title:"finding") AND (Title:"financial fraud" OR Title:"financial scam") AND (Title:"banking sector" OR Title:"banking system" OR Title:"financial sector")) OR ((Keyword:"machine learning" OR Keyword:"ml" OR Keyword:"deep learning" OR Keyword:"artificial intelligence" OR Keyword:"ai") AND (Keyword:"detection" OR Keyword:"identification" OR Keyword:"recognition" OR Keyword:"monitoring" OR Keyword:"finding") AND (Keyword:"financial fraud" OR Keyword:"financial scam") AND (Keyword:"banking sector" OR Keyword:"banking system" OR Keyword:"financial sector"))

3.2 Information Sources and Search Strategies

This research relied on academic sources of recognized international prestige, selected for their scientific rigor and for providing current, specialized, and relevant literature on artificial intelligence, machine learning, and financial fraud detection in the banking sector. The main databases consulted were: Scopus, IEEE Xplore, Web of Science, ProQuest, ScienceDirect, and ARDI. The search was structured using English descriptors to ensure broader and more relevant coverage of the results. The terms were grouped according to the research variables: the

Table 4. Results of the Quality Assessment

Ref.	Type	QA1	QA2	QA3	QA4	QA5	QA6	QA7	Ref.	Type	QA1	QA2	QA3	QA4	QA5	QA6	QA7
[1]	Journal	1	1	1	1	1	1	1	[36]	Journal	1	1	1	1	1	1	1
[2]	Journal	1	1	1	1	1	1	1	[37]	Journal	1	1	1	1	1	1	1
[3]	Journal	1	1	1	1	1	1	1	[38]	Journal	1	1	1	1	1	1	1
[4]	Journal	1	1	1	1	1	1	1	[39]	Journal	1	1	1	0	1	1	1
[5]	Journal	1	1	1	1	1	1	1	[40]	Journal	1	1	1	1	1	1	1
[6]	Journal	1	1	1	1	1	1	1	[41]	Journal	0	1	1	1	1	1	1
[7]	Journal	1	1	1	1	1	1	1	[42]	Journal	1	1	1	1	1	1	1
[8]	Journal	1	1	1	1	1	1	1	[43]	Journal	1	1	1	1	1	1	1
[9]	Journal	1	1	1	1	1	1	1	[44]	Journal	1	1	1	1	1	1	1
[10]	Journal	1	1	1	1	1	1	1	[45]	Journal	1	1	1	1	1	1	1
[11]	Journal	1	1	1	1	1	1	1	[46]	Journal	1	0	1	1	1	1	1
[12]	Journal	1	1	1	1	1	1	1	[47]	Journal	1	1	1	1	1	1	1
[13]	Journal	1	1	1	1	1	1	1	[48]	Journal	1	1	1	1	1	1	1
[14]	Journal	1	1	1	1	1	1	1	[49]	Journal	1	0	1	1	1	1	1
[15]	Journal	1	1	1	1	0	1	1	[50]	Journal	1	1	1	1	1	1	1
[16]	Journal	1	1	1	1	1	1	1	[51]	Journal	1	1	1	1	1	1	1
[17]	Journal	1	1	1	1	1	1	1	[52]	Journal	1	1	1	1	1	1	1
[18]	Journal	1	1	1	1	1	1	1	[53]	Journal	1	1	1	1	1	1	1
[19]	Journal	1	1	0	1	1	1	1	[54]	Journal	1	1	1	1	1	1	1
[20]	Journal	1	1	1	1	1	1	1	[55]	Journal	1	1	1	0	1	1	1
[21]	Journal	1	1	1	1	1	1	1	[56]	Journal	1	1	1	1	1	1	1
[22]	Journal	1	1	1	1	1	1	1	[57]	Journal	1	1	1	1	1	1	1
[23]	Journal	1	1	1	1	1	1	1	[58]	Journal	1	1	1	1	1	1	1
[24]	Journal	1	1	1	1	1	1	1	[59]	Journal	1	1	1	1	1	1	1
[25]	Journal	1	1	1	1	0	1	1	[60]	Journal	1	1	1	1	1	1	1
[26]	Journal	1	1	1	1	1	1	1	[61]	Journal	1	1	1	1	1	1	1
[27]	Journal	1	1	1	1	1	1	1	[62]	Journal	1	1	1	1	1	1	1
[28]	Journal	1	1	1	1	1	1	1	[63]	Journal	1	1	1	1	1	1	1
[29]	Journal	1	1	1	1	1	1	1	[64]	Journal	1	1	1	1	1	1	1
[30]	Journal	1	1	1	1	1	1	1	[65]	Journal	1	1	1	1	1	1	1
[31]	Journal	1	1	1	1	1	1	1	[66]	Journal	1	1	1	1	1	1	1
[32]	Journal	1	1	1	1	1	1	1	[67]	Journal	1	1	1	1	1	1	1
[33]	Journal	1	1	1	1	1	1	1	[68]	Journal	1	1	1	1	1	1	1
[34]	Journal	1	1	1	1	0	1	1	[69]	Journal	1	1	1	1	1	1	1
[35]	Journal	1	1	1	1	1	1	1	[70]	Journal	1	1	1	1	1	1	1

Independent Variable (A), related to technologies such as machine learning and artificial intelligence, and the Dependent Variable (B), focused on financial fraud detection, as shown in Table 2.

To obtain relevant information, specific search equations were designed and adapted to each of the consulted sources.

Table 3 details the search strings employed, which facilitated the systematic filtering and selection of the most pertinent studies for this research.

3.3 Identified Studies

For this research, six high-quality academic databases with strong scientific dissemination relevance were consulted: Scopus, IEEE Xplore, Web of Science, ProQuest, ScienceDirect, and ARDI. These sources enabled the collection of a broad and representative set of publications related to the subject of study, prior to applying the exclusion criteria. Figure 2 shows the distribution of documents identified in each database.

3.4 Study Selection

Exclusion Criteria (EC) were established to refine the literature and ensure the relevance of the included studies. The EC were defined according to PRISMA and Kitchenham guidelines in order to: (i) reduce bias and ensure comparability (primary studies, peer review, full-text access, and assessable language); (ii) preserve currency and external validity (recent publication window); and

(iii) ensure methodological evaluability (sufficient length, document uniqueness, and thematic consistency). The criteria were applied sequentially, and their effect on the initial universe is summarized in the PRISMA flow diagram (Figure 3).

3.5 Quality Assessment

The methodological quality of the selected studies was evaluated based on seven key criteria (QA1–QA7), defined to assess fundamental aspects of the research process and to ensure the robustness of the evidence considered. The criteria are as follows:

QA1: Are the objectives pursued by the research clearly defined?
QA2: Is the study design aligned with the achievement of these objectives?
QA3: Are the techniques employed precisely described and is their selection justified?
QA4: Were the indicators used in the study adequately assessed?
QA5: Are the methods used for data collection clearly detailed?
QA6: Is the information obtained during data collection presented sufficiently and comprehensibly?
QA7: Are relevant statistical techniques applied for data analysis, and is their selection justified?

To ensure the methodological quality of the included studies, the 70 selected papers were evaluated using the seven criteria (QA1–QA7), applying a binary scale: 1 when the study met the criterion and 0 otherwise. The results of this assessment are presented in Table 4.

As a result of the evaluation, 61 papers met all the established criteria, demonstrating adequate methodological quality, while 9 studies were excluded for presenting deficiencies in at least one of the applied criteria ([15,19,25,34,39,41,46,49,55]).

3.6 Data Extraction Strategies

Once the papers included in the analysis were defined, the most relevant information from each was organized to facilitate the review process. At this stage, data such as reference number, title, year and source of publication, countries involved in the study, ISSN, type of publication, authors, institutional affiliation, journal quartile, number of citations, abstract, keywords, discussion, and conclusions were collected.

To optimize this process, Mendeley Desktop software was employed, which allowed the documents to be organized, their metadata managed, and the required information accessed efficiently.

Figure 4 provides an overview of the working environment used during this phase.

3.7 Synthesis of Findings

In this phase, a comprehensive analysis of the papers addressing the research questions (RQ1–RQ5) was carried out. This process enabled the organization and comparison of the collected data, identifying statistically relevant patterns associated with each question.

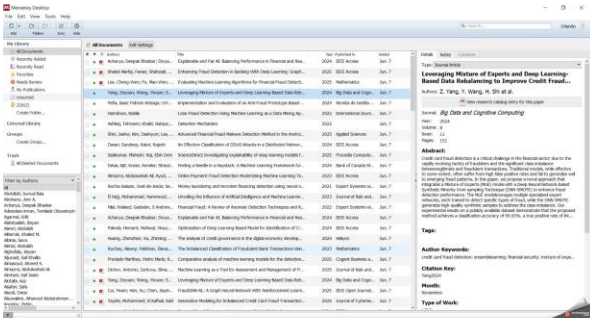
The selected studies provided valuable insights that contributed to a deeper understanding of the different research lines related to the topic, constituting an essential input for the development of this study.

4 Results and Discussion

This section presents and analyzes the results obtained, contextualizing them with the existing literature and in relation to the research objectives. The review of the 61 selected documents was conducted manually, complemented by automated processing following the stages described in Figure 5.

4.1 General Description of the Studies

Figure 6 combines a georeferenced map and a bar chart to display the distribution of papers by country of publication, offering a comparative perspective on the geographical concentration and relative contribution of each nation in research on



Mendeley Desktop

File Edit View Tools Help

Add Folders Sync Help

My Library
- All Documents
- Recently Added
- Recently Read
- Favorites
- Needs Review
- My Publications
- Unsorted
- 229521
- Create Folder...

External Library

Groups
- Create Group...

Trash
- All Deleted Documents

Filter by Authors

All
Abdullahi, Sumaiya Bala
Abohany, Amr A.
Acharya, Deepak Bhaskar
Adesokan-Imran, Tomilade Oluwatoyin
Agarwal, Udit
Alabdullah, Bayan
Alamri, Abdullah
Albarrak, Khalid M.
Albinia, Sara
Alenzi, Abdullah
Alghofaily, Bayan
Aljuraid, Saif Khalid
Almasoud, Ahmed S.
Almazroi, Abdulwahab Ali
Alnheri, Saif Saleh
Alotaibi, Aziz
Alsafari, Safa
Alsodi, Omar
Alsuwailem, Alhanouf Abdulrahman ...

All Documents | Edit Settings

Authors	Title	Year	Published In	Added
Acharya, Deepak Bhaskar; Divya...	Explainable and Fair AI: Balancing Performance in Financial and Rea...	2024	IEEE Access	Jun. 7
Khaled Alarfaj, Fawaz; Shahzadi, ...	Enhancing Fraud Detection in Banking With Deep Learning: Graph...	2025	IEEE Access	Jun. 7
Lee, Cheng-Wen; Fu, Mao-Wen; ...	Evaluating Machine Learning Algorithms for Financial Fraud Detecti...	2025	Mathematics	Jun. 7
Yang, Zeyuan; Wang, Yixuan; S...	Leveraging Mixture of Experts and Deep Learning-Based Data Reb...	2024	Big Data and Cogn...	Jun. 7
Peña, Isaac Fabricio Arteaga; Ort...	Implementation and Evaluation of an Anti-Fraud Prototype Based ...	2024	Revista de Gestão ...	Jun. 7
Hamdoun, Nabil	Loan Fraud Detection Using Machine Learning as a Data Mining Ap...	2022	International Journ...	Jun. 7
Ashfaq, Tehseen; Khalid, Rabiya;...	Detection Mechanism	2022		Jun. 7
Shin, Jaeho; Kim, Daehyun; Lee, ...	Advanced Financial Fraud Malware Detection Method in the Androi...	2025	Applied Sciences	Jun. 7
Dasari, Sandeep; Kaluri, Rajesh	An Effective Classification of DDoS Attacks in a Distributed Networ...	2024	IEEE Access	Jun. 7
Sasikumar, Mahesh; Raj, Ebin Deni	ScienceDirect Investigating explainability of deep learning models f...	2025	Procedia Compute...	Jun. 7
Desai, Ajit; Kosse, Anneke; Sharpl...	Finding a Needle in a Haystack: A Machine Learning Framework for...	2024	Bank of Canada St...	Jun. 7
Almazroi, Abdulwahab Ali; Ayub, ...	Online Payment Fraud Detection Model Using Machine Learning Te...	2023	IEEE Access	Jun. 7
Rocha-Salazar, José-de-Jesús; Se...	Money laundering and terrorism financing detection using neural n...	2021	Expert Systems wi...	Jun. 7
El Hajj, Mohammad; Hammoud, ...	Unveiling the Influence of Artificial Intelligence and Machine Learnin...	2023	Journal of Risk and...	Jun. 7
Hilal, Waleed; Gadsden, S Andrew;...	Financial Fraud: A Review of Anomaly Detection Techniques and R...	2022	Expert Systems wi...	Jun. 7
Acharya, Deepak Bhaskar; Divya...	Explainable and Fair AI: Balancing Performance in Financial and Rea...	2024	IEEE Access	Jun. 7
Paliwal, Hemant; Rishiwal, Vinay; ...	Optimization of Deep Learning-Based Model for Identification of Cr...	2024	IEEE Access	Jun. 7
Huang, Zhenzhen; Xu, Zhiming; ...	The analysis of credit governance in the digital economy develop...	2024	Heliyon	Jun. 7
Kuchay, Alexey; Feldman, Elena; ...	The Imbalanced Classification of Fraudulent Bank Transactions Usin...	2023	Mathematics	Jun. 7
Preciado Martínez, Pedro Mario; R...	Comparative analysis of machine learning models for the detection...	2025	Cogent Business a...	Jun. 7
Dichev, Antonio; Zarkova, Silvia; ...	Machine Learning as a Tool for Assessment and Management of Fr...	2025	Journal of Risk and...	Jun. 7
Yang, Zeyuan; Wang, Yixuan; S...	Leveraging Mixture of Experts and Deep Learning-Based Data Reb...	2024	Big Data and Cogn...	Jun. 7
Cai, Yiwen; Han, Xu; Chen, Jiayin...	FraudGNN-RL: A Graph Neural Network With Reinforcement Learni...	2025	IEEE Open Journal...	Jun. 7
Sayeed, Mohammed; Al Kaffash, Saad	Generative Modeling for Imbalanced Credit Card Fraud Transaction...	2025	Journal of Cyberse...	Jun. 7

Details | Notes | Contents

Type: Journal Article

Leveraging Mixture of Experts and Deep Learning-Based Data Rebalancing to Improve Credit Fraud...

Authors: Z. Yang, Y. Wang, H. Shi et al.

View research catalog entry for this paper

Journal: *Big Data and Cognitive Computing*

Year: 2024
Volume: 8
Issue: 11
Pages: 151

Abstract:

Credit card fraud detection is a critical challenge in the financial sector due to the rapidly evolving tactics of fraudsters and the significant class imbalance betweenlegitimate and fraudulent transactions. Traditional models, while effective to some extent, often suffer from high false positive rates and fail to generalize well to emerging fraud patterns. In this paper, we propose a novel approach that integrates a Mixture of Experts (MoE) model with a Deep Neural Network-based Synthetic Minority Over-sampling Technique (DNN-SMOTE) to enhance fraud detection performance. The MoE modelleverages multiple specialized expert networks, each trained to detect specific types of fraud, while the DNN-SMOTE generates high-quality synthetic samples to address the class imbalance. Our experimental results on a publicly available dataset demonstrate that the proposed method achieves a classification accuracy of 99.93%, a true positive rate of 84...

Tags:

Author Keywords:

credit card fraud detection; ensemblelearning; financial security; mixture of expe...

Citation Key:

Yang2024

Month:

November

Type of Work:

Fig. 4. Data management with Mendeley

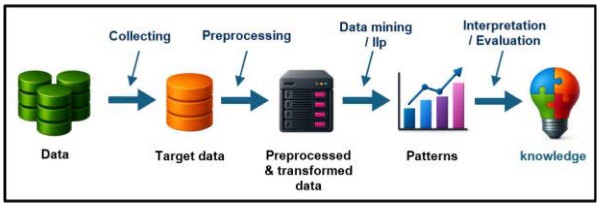


Fig. 5. Processing of selected documents

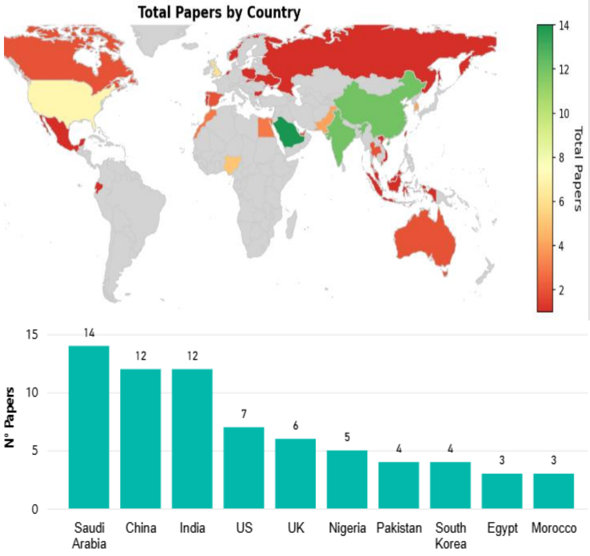


Fig. 6. Papers by country of publication

machine learning and financial fraud detection in the banking sector.

Saudi Arabia leads with 14 publications, followed by China and India with 12 each, reflecting strong interest in Asia and the Middle East.

The United States and the United Kingdom maintain significant presence, while countries such as Nigeria and Pakistan highlight the expansion of the topic into emerging regions. Overall, the data show that scientific production is no longer concentrated exclusively in Western powers.

The studies by Moura and his team [64], together with the work of Hernández Aros and his coauthors [65], coincide in noting that research on Machine Learning is concentrated in countries with advanced economies, particularly the United States, the United Kingdom, and China. Both investigations highlight that these countries lead in paper production, indicating a greater concentration of research in advanced technological areas. In turn, the research led by Gamboa-Cruzado [66] emphasizes that, in his analysis, the countries with the highest production in his field of study are similar to those identified in financial fraud detection, such as the U.S. and the U.K., which indicates a strong relationship between technology and research in these regions. Along the same lines, the group of Cárdenas-Quispe [67] also highlights that the United States leads in paper production in the field of Machine Learning, underscoring the globalization of applied methodologies.

The results demonstrate a global redistribution of knowledge, with a growing role of developing countries and increasing openness to international collaboration. This highlights the need for common methodological frameworks to strengthen fraud detection across diverse financial contexts.

Figure 7 presents, through an area chart, the evolution of the main keywords used per year in the literature on machine learning and financial fraud. This representation is justified as it allows for the identification of thematic trends and shifts in research focus over time.

The term “ml” maintains a constant and prominent presence, consolidating itself as the most representative keyword in recent years (2023–2025). “Fraud detection” shows steady growth, reaching its highest frequency in 2025, reflecting applied interest in the banking sector. “Deep learning” emerges strongly from 2023, confirming the transition toward more sophisticated techniques. “Financial fraud” remains continuous, though with less prominence, evidencing its role as a general descriptor. Finally, “ai” appears as a transversal term, with a notable resurgence in 2023 and 2025, underscoring its integrative role.

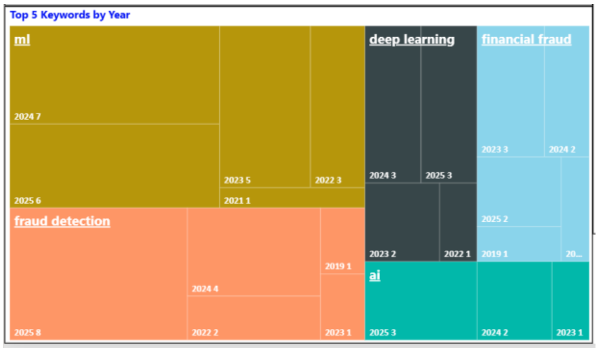


Fig. 7. Main Keywords Used by Year

As shown in the results, it is possible to identify recurrent intellectual cores within the analyzed literature, with “ml,” “deep learning,” “fraud detection,” and “financial fraud” as the main keywords, with the predominance of “ml” between 2023 and 2025. This result coincides with the findings of Hove and his team [79], who, in their bibliometric analysis, demonstrated that “machine learning” is the most frequent keyword in studies on credit card fraud detection, further highlighting its temporal evolution through a chronological occurrence map that places this term at the thematic center of the field. Similarly, Hernández Aros and his coauthors [65] reported that credit fraud detection and machine learning are central topics in recent publications, confirming the relevance of these terms in contemporary studies.

In turn, the work of Zakaria and collaborators [68] also positions machine learning as the largest and most frequent node within their co-occurrence map, reinforcing its role as the main thematic axis in financial fraud research. This finding is consistent with the study led by Lucey [83], who presents an evolutionary analysis of keywords in financial corruption research. Through a Sankey diagram, it is observed that terms such as fraud, money laundering, and artificial intelligence progressively gained prominence between 2012 and 2022, highlighting the incorporation of new thematic frontiers during the 2017–2020 period.

The analysis of keywords enables the identification of conceptual trends that dominate the field of study. Recognizing terms such as Machine Learning as a thematic core facilitates the alignment of future research with the most active lines of inquiry, thereby optimizing the relevance and potential impact of new studies.

4.2. Answers to the Research Questions

This section presents the answers to the research questions (RQ1–RQ5), highlighting the most commonly used methodological approaches, the best-performing machine learning algorithms, and the main limitations identified.

RQ1: What are the criteria for measuring the effectiveness of Machine Learning in detecting financial fraud in the banking sector?

Figure 8 and Table 5 present the main criteria used in the literature to evaluate the effectiveness of machine learning models applied to financial fraud detection in the banking sector. This representation is relevant because it allows for the identification of the most frequently used metrics and their relative weight in recent research.

The F1 Score (36.4%) is the most widely used metric, underscoring the importance of balancing precision and recall in imbalanced datasets. Sensitivity (34.5%) is also a priority, as it focuses on identifying the highest possible number of fraud cases. To a lesser extent, True Positive Rate (21.8%) and ROC AUC (7.3%) are used, reflecting the preference for practical metrics in real-world contexts.

The studies by Rao and Mandhala [69], together with the research of Hernández Aros and collaborators [65], concur that the most widely used metrics for measuring the effectiveness of Machine Learning models in financial fraud detection are precision, recall, F1-Score, and ROC AUC, highlighted for their ability to balance accuracy and fraud identification in imbalanced data contexts.

Chen and other authors [70] reinforce this idea, adding that in highly imbalanced data environments, PR AUC is more informative than ROC AUC. On the other hand, Ali and colleagues [71] emphasize that the choice of metrics depends on the type of fraud, such as credit card fraud or banking transactions, and that the use of algorithms such as Random Forest and XGBoost also influences performance evaluation. Similarly, Cárdenas and collaborators [67] highlight metrics such as high true positive rate, low false positive

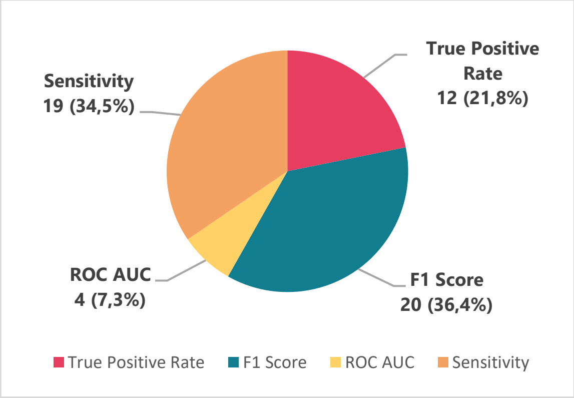


Fig. 8. Distribution of evaluation criteria

Table 5. Evaluation criteria used

Criterion	Reference	Qty. (%)
True Positive Rate	[1] [8] [12] [15] [25] [27] [29] [38] [39] [42] [50] [60]	12 (21,8)
F1 Score	[8, 9] [13] [15] [18] [25-27] [29] [35] [37] [39] [40-42] [47] [49] [52] [53] [56]	20 (36,4)
ROC AUC	[9] [15] [29] [42]	4 (7,3)
Sensitivity	[5] [10] [13] [14] [20] [21] [23-25] [29] [30] [35] [36] [39] [42] [43] [50] [56] [60]	19 (34,5)

Table 6. Programming languages used

Programming Language	Reference	Qty. (%)
Scala	[1] [2] [4] [5] [7-11] [14] [18] [19] [23-26] [28-31] [36] [37] [38] [40-43] [46] [47] [51] [52] [55] [56] [57] [59] [60]	36 (66,7)
Python	[6] [9] [11] [15] [23-25] [27] [32] [34] [40] [41] [51] [57] [59]	15 (27,8)
Java	[4] [28]	2 (3,6)
C++	[10]	1 (1,9)

rate, and Zero-Day threat prevention, which contribute to the consistency of these criteria in the literature.

The emphasis on F1 and Sensitivity can also be extended to sectors such as healthcare, telecommunications, and cybersecurity, where false negatives are critical. Moreover, their application across diverse regions and time periods would enable comparison of model effectiveness and contribute to the standardization of global practices.

RQ2: What programming languages are most commonly used in the development of Machine Learning solutions?

Table 6 and Figure 9 present the programming languages most frequently used in the development of machine learning solutions. This representation is relevant because it identifies the tools preferred by the scientific and technological community for financial fraud detection and related applications.

Scala predominates with 66.7%, reflecting its integration in big data environments such as Apache Spark. Python ranks second (27.8%), consolidating its role as a versatile language with extensive support in machine learning libraries. Java (3.6%) and C++ (1.9%) show reduced, more specialized presence. The marked difference highlights the preference for languages that combine efficiency with flexibility in handling large-scale datasets.

The findings show a relevant difference compared to previous studies. In our analysis, Scala was identified as the most frequently used language, with a presence of 59%, while in the study conducted by the group of Medarhri [72], Python was identified as the dominant language, followed by R, Java, and Matlab, with no mention of Scala. Similarly, the research of Priscilla and Padma [73] also positioned Python as the most widely used environment, with R showing a strong presence in statistical applications. In both cases, Scala does not appear as a representative language, which contrasts with our results.

This difference suggests that the studies analyzed in this review may be oriented toward contexts where distributed architectures or large-scale data processing are prioritized, rather than traditional modeling environments.

The predominance of Scala and Python can also be extended to sectors such as healthcare,

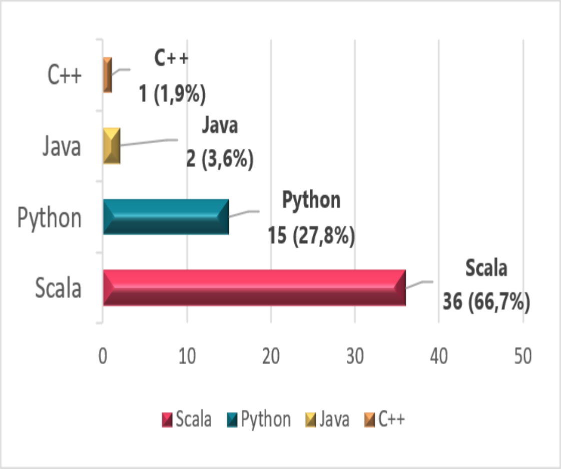


Fig. 9. Bar Chart of Programming Languages

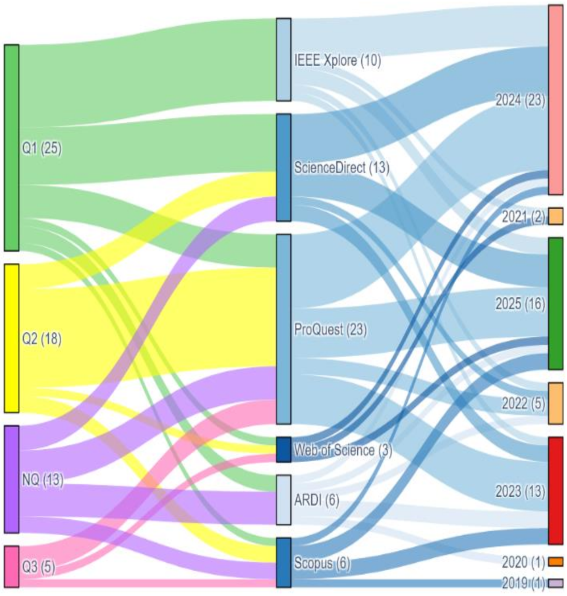


Fig. 10. Distribution of papers by Quartile, Source, and Year

telecommunications, and logistics, where large-scale data management is critical.

Their use across different regions and periods would enable the evaluation of technological evolution and the replacement of traditional languages. This reinforces the need to standardize tools that support scalable and efficient solutions in diverse business contexts.

RQ3: What are the quartile levels of the journals where research on the effect of Machine Learning in detecting financial fraud in the banking sector has been published?

Figures 10 and 11, through a Sankey diagram and a network graph, illustrate the distribution of papers according to the quartile levels of the journals in which research on machine learning and financial fraud detection has been published. This representation is relevant as it enables visualization of the concentration of publications in high-impact journals and their links with indexed databases.

The results show that most studies are concentrated in Q1 journals (25), evidencing the interest in publishing in high-impact outlets. Q2 journals (18) also represent a considerable volume, reinforcing the academic solidity of the field. In contrast, publications in Q3 (5) and non-indexed journals (13) are fewer, though they contribute to diversity. The network diagram reflects the interconnection of Q1 journals with databases such as IEEE Xplore and ScienceDirect.

The research led by Gamboa-Cruzado [66], together with the study by Cardona and collaborators [74], coincide in reporting that research on financial fraud detection through Machine Learning is published mainly in high-quartile journals (Q1 and Q2), reflecting a trend toward high-impact academic sources.

This pattern is reinforced by Zakaria and his team [68], who identified that these journals are primarily indexed in Scopus and other prestigious databases, underscoring the interest in publishing in recognized platforms. On the other hand, Nai and colleagues [75] observed that most papers are published in Q1 journals, which highlights the relevance of these metrics in the field. These conclusions strengthen the view that financial fraud detection through Machine Learning is considered a highly relevant area, with a predominant focus on high-quartile journals.

The concentration in Q1 and Q2 implies greater international recognition and potential applications in other sectors such as healthcare, energy, and telecommunications. Replicating this strategy in other geographical regions would help consolidate emerging communities. From a temporal

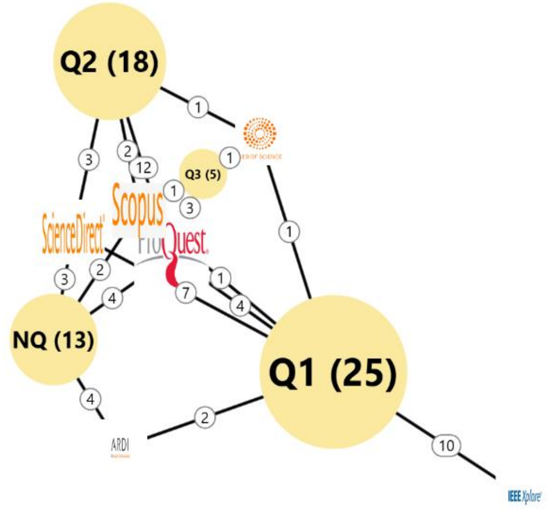


Fig. 11. Distribution of Quartiles and Information Sources.

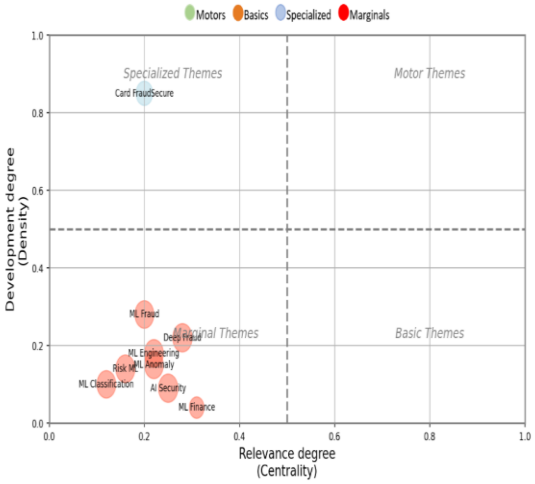


Fig. 12. Thematic Categories

Table 7. Thematic Categories

Theme	Density	Centrality	Total Citations	Total Documents	Category
Card FraudSecure	0,85	0,2	411	6	**Specialized**
ML Fraud	0,28	0,2	662	20	**Marginal**
Deep Fraud	0,22	0,28	561	13	**Marginal**
ML Engineering	0,18	0,22	656	16	**Marginal**
ML Anomaly	0,15	0,22	672	17	**Marginal**
Risk ML	0,14	0,16	672	19	**Marginal**
ML Classification	0,13	0,15	508	17	**Marginal**
AI Security	0,09	0,25	329	25	**Marginal**
ML Finance	0,04	0,31	1068	23	**Marginal**

perspective, tracking the evolution of quartiles will help assess the maturity of the field and guide new lines of research.

RQ4: What thematic categories are presented in research on Machine Learning and its impact on financial fraud detection in the banking sector?

Figure 12 and Table 7 provide an overview of the thematic categories in the literature on Machine Learning and its impact on financial fraud detection in the banking sector. These tools allow for the visualization and quantification of the centrality and density of each theme, revealing their relevance and degree of development.

The figure shows that “Card FraudSecure” is the only specialized theme, with high density (0.85) and centrality (0.2), consolidating itself as a highly developed area. In contrast, themes such as “ML Fraud” and “Deep Fraud,” with densities and centralities around 0.28 and 0.22 respectively, are marginal but supported by a considerable number of documents, suggesting emerging interest. “ML Finance” stands out for its high centrality (0.31) but low density (0.04), indicating theoretical relevance that has not yet been fully explored. The quantitative analysis also reveals that “Risk ML” and “AI Security” have the largest number of documents (25), reflecting sustained interest, though with limited development.

The studies by Moura and his team [64], together with the research of Wahib and Rohman [84], concur that financial fraud detection through Machine Learning techniques is a central area in the scientific literature, identifying categories such as intelligent fraud detection, machine learning, and financial fraud analysis as thematic pillars.

Gamboa-Cruzado and collaborators [66], through a comprehensive bibliometric analysis, highlight key areas such as advanced machine learning, neural networks, and deep learning techniques, evidencing the growing interest in sophisticated methods to improve accuracy and efficiency in fraud detection within e-commerce environments.

In turn, Laxman and his research group [78] emphasize the relevance of fraud risk management in e-commerce and the use of emerging technologies, such as artificial

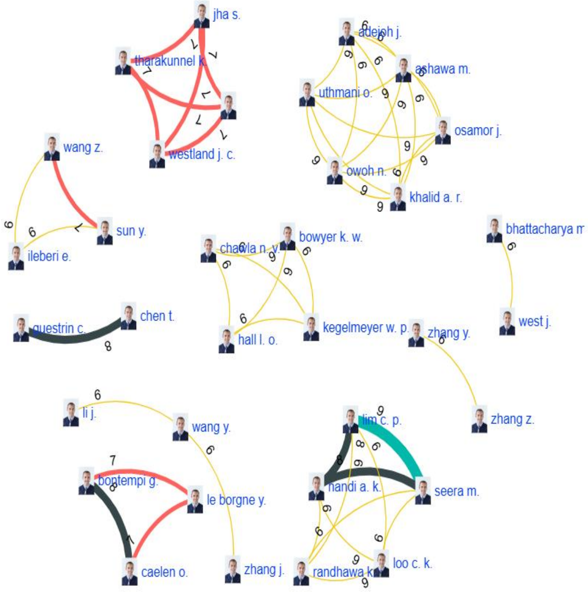


Fig. 13. Bibliometric co-citation network among authors

Table 8. Authors with the highest frequency of cocitations in the analyzed papers

Citation1	Citation2	Qty.
Lim C. P.	Seera M.	9
Bontempi G.	Caelen O.	8
Chen T.	Guestrin C.	8
Lim C. P.	Nandi A. K.	8
Nandi A. K.	Seera M.	8
Bhattacharyya S.	Jha S.	7
Bhattacharyya S.	Tharakanunnel K.	7
Bhattacharyya S.	Westland J. C.	7
Bontempi G.	Le Borgne Y.	7
Caelen O.	Le Borgne Y.	7
Jha S.	Tharakanunnel K.	7
Jha S.	Westland J. C.	7
Sun Y.	Wang Z.	7
Tharakanunnel K.	Westland J. C.	7

intelligence and blockchain, to strengthen financial security. Lucey and colleagues [83] contribute a complementary perspective by identifying financial corruption as a phenomenon closely linked to fraudulent activities, stressing the need to address these issues from a multidisciplinary perspective that includes network analysis and collaborations among researchers. These studies combine advances in Machine Learning with security and collaboration to enhance the detection and prevention of financial fraud.

The thematic diversity demonstrates potential for multisectoral applications, such as marketing and cybersecurity. Geographically, emphasis may vary, adapting to local regulations and market needs. Within 3 to 5 years, it is anticipated that "Card FraudSecure" will lead new guidelines, while "ML Finance" may evolve toward more integrated approaches driven by technological developments and emerging needs in fraud detection.

RQ5: Who are the authors of the references that most frequently present co-citations in research on Machine Learning and its impact on financial fraud detection in the banking sector?

Figure 13 and Table 8 present the co-citation network among key authors in research on machine learning applied to banking fraud. This visualization is useful for identifying methodological clusters and sub-communities that structure the field.

The strongest link is Lim C. P.–Seera M. (9), and the triangle Lim–Nandi–Seera (8 each) evidences a stable cluster oriented toward classification and applied systems. Bontempi–Caelen–Le Borgne (8–7–7) form a second methodological nucleus associated with statistical learning and data streams. Chen–Guestrin (8) confirms the technical centrality of XGBoost as a cross-cutting reference in the studies. Pairs such as Bhattacharyya–Jha–Tharakanunnel–Westland (7) and Sun–Wang (7) show regional sub-networks and historical continuity of joint citation.

Compared with the results obtained in this review, where authors such as Lim C. P. and Seera M. stand out with 9 co-citations, both coinciding and divergent patterns are identified in other recent studies. For instance, in [78], strong co-citation was observed among authors Caelen O., Bontempi G., and Li Z., who present the most significant links within a network composed of 151 authors, structured into four clusters. In [79], the predominance of Caelen O. is highlighted, who demonstrates strong link strength and collaborates closely with authors such as He-Guelton L., Bontempi G., Portier P., and Oble F., all of whom are central nodes in co-citation maps within the domain of credit card fraud detection. In [80], the most cited author is Kauffman R. J., with 12 publications and more than 2,000 citations, followed by Asongu S. and Karjaluoto H., who represent the most influential nodes within a network comprising more than 100 authors across five main clusters.

In the work of [81], five foundational knowledge clusters in financial research with AI are identified, the most prominent being those related to bankruptcy prediction techniques and machine learning (red nodes), and fintech ecosystems (dark green nodes).

Similarly, in the review conducted by Thakkar and collaborators [85], the central role of Khoshgoftaar T. M. is confirmed, who is highly co-cited alongside Najafabadi M. M. and Johnson J. M., consolidating his influence in studies on fraud detection through deep learning.

These nuclei can guide focused reviews and transferable benchmarks to other sectors (insurance, e-commerce, telecommunications) and business areas (risk, compliance, payments). Replicating the analysis in different geographies would make it possible to contrast co-citation patterns and the maturity of local communities. A longitudinal follow-up would show the evolution of methodological poles (e.g., XGBoost) and the emergence of new authors, facilitating collaboration agendas and technology transfer.

5 Conclusions and Future Research

In RQ1, effectiveness in detection relies on metrics sensitive to imbalance, with F1-score and sensitivity standing out for their ability to balance precision and recall in low-prevalence scenarios, while ROC AUC is less frequently used, as cost-sensitive indicators and the reduction of false negatives are prioritized. In summary, the F1–sensitivity pair guides more robust thresholds and early alerts, and metrics should be selected based on their operational impact—such as loss recovery and regulatory compliance—rather than global averages.

In RQ2, Scala predominates in production environments due to its integration with distributed processing and streaming (e.g., Spark), whereas Python leads in prototyping thanks to its library ecosystem and rapid experimentation, thereby consolidating a polyglot strategy where Scala is geared toward scalability and real-time applications, Python toward research and analysis, and Java/C++ toward integration niches or specific performance needs, maximizing interoperability between analytics and large-scale computing.

In RQ4, the thematic map reveals a field without motor themes and dominated by marginal clusters, reflecting a consolidation phase; in this context, Card FraudSecure emerges as a specialized theme with high density and peripheral centrality—useful but limited—while ML Finance, with high centrality and low density, appears as a promising but still developing nucleus.

This requires prioritizing trajectories that strengthen the density of medium-to-high centrality topics so they can become structuring axes of the field. Finally, in RQ5, the co-citation network shows stable methodological nuclei, such as the Lim–Seera or Bontempi–Caelen–Le Borgne associations, which organize much of the referencing, and also confirms the cross-cutting centrality of XGBoost (Chen–Guestrin), suggesting trajectories of standardization in metrics, data, and pipelines, along with knowledge governance that accelerates convergence and ensures reproducibility in regulated environments.

Altogether, the synthesis of these RQs confirms that useful performance in banking depends on the combination of cost-sensitive, risk-oriented metrics, languages aligned with scalability, thematic agendas with greater maturity, and well-connected methodological nuclei.

For future research, it is necessary to develop standardized datasets and cost-sensitive multi-metric evaluations in both batch and streaming contexts, linking F1–sensitivity with avoided losses; to study hybrid Python–Scala architectures and reproducible MLOps frameworks with explainability and auditability for different regulatory regimes; and to strengthen the density of central themes (e.g., ML Finance) through interregional collaborations and longitudinal follow-ups that integrate co-citation, thematic mapping, and field validation.

References

1. **Acharya, D. B., Divya, B. Kuppan, K. (2024).** Explainable and fair AI: Balancing performance in financial and real estate machine learning models. IEEE Access, Vol. 12, doi: 154022–154034.
2. **Da Silva Lopes, T. (2020).** International journal of management and business. Oxford Research Encyclopedia of Business and Management.
3. **Alenizi, A., Mishra, S. Baihan, A. (2024).** Enhancing secure financial transactions through the synergy of blockchain and artificial intelligence. Ain Shams Engineering Journal. doi: 10.1016/j.asej.2024.102733.
4. **Aljunaid, S. K., Almheiri, S. J., Dawood, H. (2025).** Secure and transparent banking: Explainable AI-driven federated learning model for financial fraud detection. Journal of Risk and Financial Management. doi: 10.3390/jrfm18040179.
5. **Anitha, V. (2023).** Online payment fraud detection model using machine learning techniques. International Journal for Research in Applied Science and Engineering Technology.
6. **Alsuwailem, A. A. S., Salem, E. Saudagar, A. K. J. (2023).** Performance of different machine learning algorithms in detecting financial fraud. Computational Economics.

   doi: 10.1109/ACCESS.2023.3339226
7. **Saravanan, K. (2022).** A machine learning and blockchain based efficient fraud detection mechanism. International Journal of Computer and Electrical Engineering.
8. **Binsawad, M. (2025).** Enhanced financial fraud detection using an adaptive voted perceptron model with optimized learning and error reduction. Electronics. doi: 10.33390/electronics14091875.
9. **Btoush, E., Zhou, X., Gururajan, R. (2025).** Achieving excellence in cyber fraud detection: A hybrid ML+DL ensemble approach for credit cards. Applied Sciences. doi: 10.3390/app15031081
10. **Chen, Z., Zhang, S., Zeng, X. (2023).** Parallel path detection for fraudulent accounts in banks based on graph analysis. PeerJ Computer Science. doi: 10.7717/peerj-cs.1749
11. **Cui, Y., Han, X., Chen, J. (2025).** Fraud GNN-RL: A graph neural network with reinforcement learning for adaptive financial fraud detection. IEEE Open Journal of the Computer Society. doi: 10.1109/OJCS.2025.3543450
12. **Dantas, R. M., Firdaus, R., Jaleel, F. (2022).** Systemic acquired critique of credit card deception exposure through machine learning. Journal of Open Innovation: Technology, Market, and Complexity. doi: 10.3390/joitmc8040192
13. **Dasari, S. Kaluri, R. (2024).** An effective classification of DDoS attacks in a distributed network by adopting hierarchical machine learning and hyperparameters optimization techniques. IEEE Access. doi: 10.1109/ACCESS.2024.3352281
14. **Desai, A., Kosse, A. Sharples, J. (2024).** Finding a needle in a haystack: A machine learning framework for anomaly detection in payment systems. The Journal of Finance and Data Science.
15. **Detthamrong, U., Chansanam, W., Boongoen, T. (2024).** Enhancing fraud detection in banking using advanced machine learning techniques. Journal of Information Systems Engineering and Management. doi: 10.32479/ ijefi.16613
16. **Dichev, A., Zarkova, S. Angelov, P. (2025).** Machine learning as a tool for assessment and management of fraud risk in banking transactions. Journal of Risk and Financial Management. doi: 10.3390/jrfm1803130
17. **El Hajj, M., Hammoud, J. (2023).** Unveiling the influence of artificial intelligence and machine learning on financial markets: A comprehensive analysis of AI applications in trading, risk management, and financial operations. Journal of Risk and Financial Management.
18. **Rho, C., Fernández, R., Palma, B. (2021).** A sentiment-based risk indicator for the Mexican financial sector. Latin American Journal of

Central Banking. doi: 10.1016/j.latcb.2021.100036

19. **Gandhi, H., Tandon, K., Gite, S. (2024).** Navigating the complexity of money laundering: Anti–money laundering advancements with AI/ML insights. International Journal on Smart Sensing and Intelligent Systems.

20. **Hamdoun, N. (2022).** Loan fraud detection using machine learning as a data mining approach. International Journal of Data Analytics. doi: 10.4018/IJDA.309096

21. **Hilal, W., Gadsden, S. A., Yawney, J. (2022).** Financial fraud: A review of anomaly detection techniques and recent advances. Expert Systems with Applications. doi: 10.1016/j.eswa.2021.116429

22. **Huang, Z., Xu, Z., Wang, X. (2024).** The analysis of credit governance in the digital economy development under artificial neural networks. Heliyon. doi: 10.1016/j.heliyon.2024.e39286.

23. **Huot, C., Heng, S., Kim, T.-K. (2024).** Quantum autoencoder for enhanced fraud detection in imbalanced credit card dataset. IEEE Access. doi: 10.1109/ ACCESS.2024.3496901.

24. **Gupta, S., Patel, S., Kumar, S. (2024).** A comprehensive machine learning framework for anomaly detection in credit card transactions. International Journal of Innovative Research in Computer Science and Technology. doi: 10.14569/IJACSA. 2024.0150688.

25. **Karnavou, E., Cascavilla, G., Marcelino, G., Geradts, Z. (2025).** I know you're a fraud: Uncovering illicit activity in a Greek bank transactions with unsupervised learning. Elsevier. doi: 10.1016/j.eswa.2025.128148.

26. **Alarfaj, F. K., Shahzadi, S. (2025).** Enhancing fraud detection in banking with deep learning: Graph neural networks and autoencoders for real-time credit card fraud prevention. IEEE Access. doi: 10.1109/ACCESS.2024. 3466288.

27. **Khang, V. H., Anh, C. T., Thuan, N. D. (2023).** Detecting fraud transaction using ripper algorithm combines with ensemble learning model. International Journal of Advanced Computer Science and Applications. doi: 10.14569/IJACSA.2023.0140438.

28. **Krishna, V. R., Boddu, S. (2023).** Financial fraud detection using improved artificial humming bird algorithm with modified extreme learning machine. International Journal on Recent and Innovation Trends in Computing and Communication. doi: 10.17762/ijritcc. v11i5s.6593

29. **Le, T.-T.-H., Hwang, Y., Kang, H. (2024).** Robust credit card fraud detection based on efficient Kolmogorov-Arnold network models. IEEE Access. doi: 10.1109/ACCESS.2024.3485200.

30. **Lee, C.-W., Fu, M.-W., Wang, C.-C. (2025).** Evaluating machine learning algorithms for financial fraud detection: Insights from Indonesia. Mathematics. doi: 10.3390/math13040600.

31. **Lee, J., Jung, D., Moon, J. (2025).** Advanced R-GAN: Generating anomaly data for improved detection in imbalanced datasets using regularized generative adversarial networks. Alexandria Engineering Journal. doi: 10.1016/j.aej.2024.10.084.

32. **Li, B., Yen, J., Wang, S. (2024).** Uncovering financial statement fraud: A machine learning approach with key financial indicators and real-world applications. IEEE Access. doi: 10.1109/ACCESS.2024.3520249

33. **Li, Y., Fu, B., Tong, Y. (2024).** Abnormal detection of financial fraud in listed companies based on deep learning. Procedia Computer Science. doi: 10.1016/j.procs.2024.08.112

34. **Maashi, M., Alabduallah, B. & Kouki, F. (2023).** Sustainable financial fraud detection using Garra Rufa fish optimization algorithm with ensemble deep learning. Sustainability. doi: 10.3390/su151813301.

35. **Miao, Z. (2024).** Financial fraud detection and prevention. Financial Fraud Prevention and Detection.

36. **Oyekunle, S. M., Popoola, A. D., Kolo, F. H. O., (2025).** Intelligent fraud prevention information banking: A data governance-

centric approach using behavioural biometrics. Asian Journal of Research in Computer Science. doi: 10.9734/ajrcos/2025/v18i5672.

37. **Mosa, D. T., Sorour, S. E., Abohany, A. A. (2024).** CCFD: Efficient credit card fraud detection using meta-heuristic techniques and machine learning algorithms. Mathematics. doi :10.3390/math12142250

38. **Murugan, M. S., T., S. K. (2023).** Large-scale data-driven financial risk management & analysis using machine learning strategies. Measurement: Sensors. doi: 10.1016/j.measen.2023.100756

39. **Mytnyk, B., Tkachyk, O., Shakhovska, N., (2023).** Application of artificial intelligence for fraudulent banking operations recognition. Big Data and Cognitive Computing. Doi: 10.3390/bdcc7020093

40. **Oyewola, D. O., Omotehinwa, T. O., Dada, E. G. (2023).** Consumer complaints of consumer financial protection bureau via two-stage residual one-dimensional convolutional neural network (TSR1DCNN). Data and Information Management. doi: /10.1016/j.dim.2023.100046

41. **Palivela, H., Rishiwal, V., Bhushan, S., (2024).** Optimization of deep learning-based model for identification of credit card frauds. IEEE Access. doi: 10.1109/ACCESS. 2024.3440637

42. **Patel, S. K. & Panday, D. (2024).** Optimizing credit card fraud detection: A genetic algorithm approach with multiple feature selection methods. ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal. doi: 10.1109/ACCESS.2024.3440637

43. **Paul, E. O., Callistus, O., Somtobe, O., Esther, T. (2023).** Cybersecurity strategies for safeguarding customer's data and preventing financial fraud in the United States financial sectors. International Journal on Soft Computing. doi: 10.5121/ijsc.2023.14301.

44. **Peña, I. P. A., Ortega-Castro, J. C. (2024).** Implementation and evaluation of an anti-fraud prototype based on generative artificial intelligence for the Ecuadorian financial sector. Revista de Gestão Social e Ambiental.

45. **Polireddi, N. S. A. (2024).** An effective role of artificial intelligence and machine learning in banking sector. Measurement: Sensors. doi: 10.1016/j.measen.2024.101135

46. **Pranto, T. H., Hasib, K. T. A. M., Rahman, T., Haque, A. B., Islam, A. K. M. N. & Rahman, R. M. (2022).** Blockchain and machine learning for fraud detection: A privacy-preserving and adaptive incentive based approach. IEEE Access.

47. **Martínez, P. M. P., Forradellas, R. F. R., Gallastegui, L. M. G. & Alonso, S. L. N. (2025).** Comparative analysis of machine learning models for the detection of fraudulent banking transactions. Cogent Business and Management.

48. **Rocha-Salazar, J.-d.-J., Segovia-Vargas, M.-J. & Camacho-Miñano, M.-d.-M. (2021).** Money laundering and terrorism financing detection using neural networks and an abnormality indicator. Expert Systems with Applications.

49. **Ruchay, A., Feldman, E., Cherbadzhi, D. & Sokolov, A. (2023).** The imbalanced classification of fraudulent bank transactions using machine learning. Mathematics.

50. **Sadgali, I., Sael, N. & Benabbou, F. (2019).** Performance of machine learning techniques in the detection of financial frauds. Procedia Computer Science.

51. **Sasikumar, M. & Raj, E. D. (2025).** Investigating explainability of deep learning models for sequential data on stock price prediction. Procedia Computer Science.

52. **Shin, J., Kim, D. & Lee, K. (2025).** Advanced financial fraud malware detection method in the Android environment. Applied Sciences.

53. **Sorour, S. E., AlBarrak, K. M., Abohany, A. A. & El-Mageed, A. A. A. (2024).** Credit card fraud detection using the brown bear optimization algorithm. Alexandria Engineering Journal.

54. **Srokosz, M., Bobyk, A., Ksiezopolski, B. & Wydra, M. (2023).** Machine-learning-based scoring system for antifraud CISIRTs in banking environment. Electronics.

55. **Sruthi, S., Emadaboina, S. & Jyotsna, C. (2024).** Enhancing credit card fraud detection: An ensemble machine learning approach. 2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS).

56. **Tayebi, M. & El Kafhali, S. (2025).** Generative modeling for imbalanced credit card fraud transaction detection. Journal of Cybersecurity and Privacy.

57. **Lakshminadh, P. (2024).** Financial fraud detection using value-at-risk with machine learning in skewed data. Journal of Engineering Sciences.

58. **Krishnamoorthy, M. V. (2025).** Data obfuscation through latent space projection for privacy-preserving AI governance: Case studies in medical diagnosis and finance fraud detection. JMIRx Med.

59. **Wu, Y., Wang, L., Li, H. & Liu, J. (2025).** A deep learning method of credit card fraud detection based on continuous-coupled neural networks. Mathematics.

60. **Yang, Z., Wang, Y., Shi, H. & Qiu, Q. (2024).** Leveraging mixture of experts and deep learning-based data rebalancing to improve credit fraud detection. Big Data and Cognitive Computing.

61. **Zhu, S., Wu, H., Ngai, E. W. T., Ren, J., He, D., Ma, T. & Li, Y. (2024).** A financial fraud prediction framework based on stacking ensemble learning. Systems.

62. **Kitchenham, B. & Charters, S. (2007).** Guidelines for performing systematic literature reviews in software engineering. *Technical Report EBSE-2007-01*, School of Computer Science and Mathematics, Keele University.

63. **Petersen, K., Feldt, R., Mujtaba, S. & Mattsson, M. (2008).** Systematic mapping studies in software engineering. 12th International Conference on Evaluation and Assessment in Software Engineering (EASE), 68–77.

64. **Moura, L., Barcaui, A. & Payer, R. (2024).** AI and financial fraud prevention: Mapping the trends and challenges through a bibliometric lens. Journal of Risk and Financial Management, 17(1).

65. **Hernández Aros, L., Moreno Hernández, J., Bustamante Molano, L. X. & Gutiérrez Portela, F. (2024).** Financial fraud detection through the application of machine learning techniques: A literature review. Humanities and Social Sciences Communications, 11(1), 1130.

66. **Gamboa-Cruzado, J., Mosqueira-Cerda, T., Torre Camones, A., Quispe Mendoza, R., Navarro Raymundo, A. F., Jiménez García, J. & López-Ramírez, B. C. (2025).** Exploring the influence of machine learning in e-Commerce: A systematic and bibliometric review. Computación y Sistemas, 29(2), 925–953.

67. **Cárdenas-Quispe, A., Vergaray-Mezarina, R. & Gamboa-Cruzado, J. (2021).** Machine learning for malware detection on Android: Systematic literature review. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, (E45)*, 318–331.

68. **Zakaria, N., Sulaiman, A., Min, F. S. & Feizollah, A. (2023).** Machine learning in the financial industry: A bibliometric approach to evidencing applications. Cogent Social Sciences, 9(2).

69. **Rao, R. & Mandhala, V. N. (2024).** Unveiling financial fraud: A comprehensive review of machine learning and data mining techniques. Engineering Systems and Information Journal, 29(6), 2309-2334.

70. **Chen, Y., Zhao, C., Xu, Y. & Nie, C. (2025).** Year-over-year developments in financial fraud detection via deep learning: A systematic literature review. IEEE Access.

71. **Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., Elhassan, T., Elshafie, H. & Saif, A. (2022).** Financial fraud detection based on machine learning: A systematic literature review. Applied Sciences, 12, 9637.

72. **Medarhri, I., Derouiche, L. & Idri, A. (2022).** A systematic mapping study on machine learning techniques for credit card fraud detection. Procedia Computer Science, 201, 608–615.

73. **Priscilla, A. V. & Padma, M. (2021).** A bibliometric analysis on machine learning research using Scopus data from 2005 to 2020. Turkish Journal of Computer and Mathematics Education, 12(10), 7145–7154.
74. **Cardona, L. F., Guzmán-Luna, J. A. & Restrepo-Carmona, J. A. (2024).** Bibliometric analysis of the machine learning applications in fraud detection on crowdfunding platforms. Journal of Risk and Financial Management, 17(8), 352.
75. **Nai, R., Sulis, E. & Meo, R. (2022).** Public procurement fraud detection and artificial intelligence techniques: A literature review. CEUR Workshop Proceedings.
76. **Rojas, J., Gamboa-Cruzado, J. & de la Cruz Vélez, P. (2023).** Systematic literature review on machine learning and its impact on APIs deployment. Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería de Sistemas e Informática.
77. **Aparcana-Tasayco, A. & Gamboa-Cruzado, J. (2022).** Machine learning for management in software-defined networks: A systematic literature review. International Journal of Computer Applications, 184(34), 1–10.
78. **Laxman, V., Ramesh, N., Prakash, S. K. J. & Aluvala, R. (2024).** Emerging threats in digital payment and financial crime: A bibliometric review. Journal of Digital Economy, 3, 205–222.
79. **Hove, D., Olugbara, O. & Singh, A. (2024).** Bibliometric analysis of recent trends in machine learning for online credit card fraud detection. Journal of Scientometric Research, 13(1), 43–57.
80. **Dirie, A. N. (2024).** Exploring the role and application of artificial intelligence and machine learning in digital financial inclusion: Identifying key themes and trends through bibliometric analysis in the era of the digital revolution and technological advancement. International Journal of Engineering Trends and Technology, 72(7), 266–277.
81. **Vuković, D. B., Dekpo-Adza, S. & Matović, S. (2025).** AI integration in financial services: A systematic review of trends and regulatory challenges. Humanities & Social Sciences Communications, 12(1), 562.
82. **Gamboa-Cruzado, J., Crisostomo-Castro, R., Vila-Buleje, J., López-Goycochea, J. & Nolasco Valenzuela, J. (2024).** Heart attack prediction using machine learning: A comprehensive systematic review and bibliometric analysis. *Journal of King Saud University - Computer and Information Sciences, 35*(7), 101269.
83. **Lucey, B. M., Kumar, S. & Sureka, R. (2023).** Corruption in finance research: The state of art and future research agenda. Journal of Economic Criminology, 1, 100001.
84. **Wahib, M. F. N. & Rohman, A. (2024).** A bibliometric analysis of the financial fraud detection literature from 2004 to 2024. Journal of Economics, Finance and Management Studies, 7(9), 5855–5867.
85. **Thakkar, H., Datta, S., Bhadra, P., Barot, H. & Jadav, J. (2025).** Artificial intelligence and machine learning in fraud detection: A comprehensive bibliometric mapping of research trends and directions. Annals of Library and Information Studies, 72(2), 138–150.

Article received on 12/02/2025; accepted on 03/07/2025.
**Corresponding author is Francisco A. Castillo-Velázquez.*